

**AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT APPLICATIONS**

I, Michael Perrella, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications for each of two search warrants, as follows:

a. A search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure authorizing the examination of property, one Samsung Note 8, Model # SM-N950U, described in Attachment A (hereafter “the Device”), stored in evidence storage at the U.S. Probation Office, 55 Pleasant Street, Room 211, Concord, NH, to search for and to seize information further identified in Attachment B. I submit, based on the facts as set out below, that there is probable cause to believe that the Device contains evidence of Possession of Child Pornography, in violation of 18 U.S.C. § 2252.

b. A search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Fed. R. Crim. P. 41 authorizing the search of a certain Dropbox account (hereafter “the Account”), associated with the Dropbox username “scurrier” and the e-mail address “scurrier [REDACTED]@gmail.com” that is stored at premises controlled by Dropbox Inc., which is headquartered at San Francisco, California, as described in Attachment A. I submit, based on the facts as set out below, that there is probable cause to believe that records and other information associated with this account contain evidence and fruits, and are instrumentalities of, Possession of Child Pornography, violation of 18 U.S.C. § 2252.

2. I am a Special Agent (SA) of the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I am currently assigned to the HSI Resident Agent in Charge, Manchester, New Hampshire and have been employed in that capacity since October 2017. Prior to this assignment, I was assigned to the Immigration and Customs Enforcement, Office of Professional Responsibility, Resident Agent in Charge, Portsmouth, NH, since July 2006; I served at the ICE-HSI Special Agent in Charge, Boston, Massachusetts from March 2003 to July 2006; and served in several capacities with the legacy Immigration and Naturalization Service (INS) to include Special Agent and U.S. Border Patrol Agent from 1996 to 2003. My current duties as a Special Agent include investigating violations of possession, distribution, receipt and production of child pornography, and I am empowered to investigate and make arrests for offenses involving the aforementioned offenses. As an SA with HSI, I have received specialized training on how to conduct these investigations and am familiar with and have received training regarding federal laws relating to, among other things, the unlawful possession, distribution, and receipt of child pornography, 18 U.S.C. § 2252, Possession of Child Pornography. I have participated in child pornography investigations and have assisted in the execution of federal search warrants in connection with those investigations.

3. I am a “Federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The information contained in this affidavit is based, in part, on my personal knowledge and information I have received from the U.S. Probation Office. This affidavit is submitted for the purpose of establishing probable cause to support the issuance of search

warrants. While this affidavit contains facts relevant to the requested search warrants, it does not include each and every fact known to me, or to other investigators, concerning this investigation. That being said, I am not aware of any information that would contradict the information provided here, or that would suggest that probable cause does not exist.

JURISDICTION FOR SEARCH WARRANTS

5. This Court has jurisdiction to issue the requested search warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a “district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(ii).

6. The investigation involves offenses within the jurisdiction and venue of the United States District Court for the District of New Hampshire. *See* 18 U.S.C. § 3237(a); *see also* 18 U.S.C. §§ 3231 and 3232. Moreover, as the affidavit sets out, the Account discussed in this affidavit was accessed from the District of New Hampshire by an individual utilizing the Account for that which this warrant is being sought.

RELEVANT STATUTES

7. This investigation concerns alleged violations of 18 U.S.C. § 2252, Possession of Child Pornography, which prohibits a person from knowingly possessing or accessing images of sexually explicit conduct, as defined at 18 U.S.C. § 2256(2)(A), with the intent to view them, as well as transporting or receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (i.e., child pornography). The following definitions apply to this Search Warrant Application:

a. **“Child Pornography”**, as used herein, is defined in Title 18 United States Code § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. **“Minor”** means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

c. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

PROBABLE CAUSE

8. On March 12, 2018, United States Probation Officer (USPO) Matthew Farwell conducted an unannounced home visit at the residence of Scott Currier, at [REDACTED] White Mountain Highway, Milton, NH 03851. Currier is currently serving a term of supervised release resulting from a 2009 conviction in the District of New Hampshire for money laundering. He is also a registered sex offender, following an April 5, 2000 conviction in Strafford County, NH, Superior Court, for aggravated felonious sexual assault on a female child, age eight to twelve. Currier's federal supervision is subject to the following special conditions: (1) he shall neither possess nor have under his control any material depicting sexually explicit conduct, as that term is defined in

18 U.S.C. § 2256(2), involving **adults or children** (emphasis added), including but not limited to any “matter” obtained through access to any computer or any material linked to computer access or use; (2) he is barred from the use of the internet and all media devices with interactive computer service, without prior approval of the probation officer. Before this date, Currier had not received any such approval.

9. On arrival at Currier’s residence, USPO Farwell attempted to call the phone number previously provided by Currier to ask him to answer the door. The phone went directly to voicemail, indicating that the phone might be turned off.

10. USPO Farwell then knocked on the door and heard shuffling sounds, as if furniture was being moved around inside the residence. It took approximately two minutes for Currier to finally come to the door. When he did, he was not wearing a shirt, and claimed that he was about to get in the shower. During initial conversation with USPO Farwell, Currier claimed that his wife had moved out and that she is currently living in Sanford, ME, and that his landlord was in the process of finding him a roommate. Currier also said that he was currently employed at Madeline’s Event Central in Portsmouth, NH. USPO Farwell continued to walk through the apartment and did not observe any weapons or other contraband.

11. While in Currier’s bedroom, USPO Farwell heard what he believed to be an “alert chime” indicating that a cellular phone had received a text or an e-mail. His own phone was in silent mode, so he knew that it was not an alert from his phone. USPO Farwell asked Currier to produce his phone. Currier told USPO Farwell that his phone was not working, because the battery was dead. USPO Farwell then asked Currier what the chime was, and if Currier was in possession of any other devices capable of accessing the internet. Currier denied that he was in

possession of any such devices, but admitted to recently obtaining a new cellular phone, and said that he had intended to bring it to USPO Farwell to discuss internet monitoring.

12. USPO Farwell asked to see Currier's phone, and Currier retrieved the Device from between the mattress and box spring of his bed. USPO Farwell asked Currier why he did not notify him of the Device as required by Supervised Release conditions, instead of engaging in conduct that was in violation of those conditions. Currier explained that he was afraid to trust the probation office and to have monitoring software installed on the Device, which Currier knew would be required of any device he might possess that could access the internet. Currier claimed that his dishonesty was a result of his time in prison and personal embarrassment. Currier further explained that he was accustomed to hiding things, and had engaged in similar behavior while on state probation.

13. USPO Farwell asked Currier if there were any sexually explicit images on the Device, which as noted above at paragraph 8 would be a violation of his Supervised Release conditions. Currier answered that there were such images on the Device, including pictures of himself: (a) in the nude (b) wearing women's lingerie. (c) engaging in sexual acts with his wife, (d) engaging in sexual acts with other women, as well as (e) pictures of his wife engaging in sexual acts with other men.

14. Currier also admitted to storing and backing up images on Dropbox, a commonly used, cloud based, storage medium for digital files, although he did not expressly state that these images were the same images referenced in paragraph 13. Currier denied engaging in any inappropriate behavior with minors, and further denied possessing any sexually explicit images of minors. Currier acknowledged that, by possessing the images referenced above at paragraph 13, he had violated his treatment contract.

15. USPO Farwell asked Currier if he had disclosed this behavior to his counselor. To which Currier said he had not, and expressed shame and embarrassment at the thought of disclosing his behavior. Currier further told USPO Farwell that he has experienced thoughts and feelings that were not “normal” since he went to prison in 2001. USPO Farwell allowed Currier to retain custody of the Device but instructed him not to wipe the Device or remove any software or images without USPO Farwell’s permission.

16. Currier told USPO Farwell that he had been in possession of the Device since October 2017 and the phone number is (603) [REDACTED] 7818.

17. Nine days later, on March 21, 2018, as directed by USPO Farwell, Currier reported to the U.S. Probation Office in Concord, NH with the Device. USPO Farwell instructed Currier to complete a Computer Usage Questionnaire used regularly by the US Probation Office in situations where Supervisees possess computers and other internet capable devices. The form asks for items including usernames and account passwords for email, social networking and remote storage sites.

18. During this office visit, USPO Farwell told Currier that he, Farwell, would have monitoring software installed on the Device, after which Currier would be required to return again to the probation office to retrieve the Device. Currier indicated that he understood and would comply with USPO Farwell’s instructions. USPO Currier surrendered the Device and USPO Farwell provided Currier with a property receipt. Currier was then escorted out of the probation office.

19. After Currier left, USPO Farwell conducted a brief, cursory examination of the Device based on his reasonable suspicion that Currier had used the Device to violate the special conditions of his supervision barring him from possessing sexually explicit materials, and from

use of the internet and all media devices with interactive computer service without prior approval by his probation officer. Farwell noticed the application Dropbox, which he knew to be an internet, cloud based, storage application that allows the user to store and share files with others. USPO Farwell explained that although Currier had provided a password for his Dropbox account, no password was needed to gain access to the Dropbox account on Currier's Device.

20. USPO Farwell opened the Dropbox application and determined that files had been uploaded to the Account on Currier's Device beginning in Fall 2016, approximately a year before the time Currier had advised he had obtained the Device. *See* ¶ 16 *supra*. On viewing the files in the Account, USPO Farwell saw nude images of Currier, Currier's wife, and other people with whom Currier and his wife were engaged in sexual acts, consistent with the descriptions Currier had provided of images he said were stored on his phone.

21. However, USPO Farwell also found a video file showing an adult female and what he observed to be a pre-pubescent female engaged in sexual acts, specifically the pre-pubescent female appeared to be sucking the breast of the adult female, and the adult female appearing to guide the pre-pubescent female's head toward her groin as a prelude to the minor performing oral sex on the adult female, inconsistent with Currier's earlier denials of not possessing sexually explicit images of minors. On observing the file referenced in this paragraph, USPO Farwell immediately notified his supervisor and Assistant United States Attorney Mark Zuckerman about what he had seen.

22. USPO Farwell then placed the Device in airplane mode, turned off its Wi-Fi capability, shut it down, placed it in a tamper resistant evidence bag, and locked it in the Probation office's evidence locker.

23. On March 21, 2018, I made contact, via telephone, with USPO Farwell about what he had reported to AUSA Zuckerman. USPO Farwell provided a brief verbal synopsis of the events outlined above, and provided, via email, a copy of the Computer Usage Questionnaire that Currier had filled out earlier that day.

24. I reviewed the “Computer Usage Questionnaire” provided by USPO Farwell. Section 2, page 2 of the document specifically asks the Supervisee to list profiles with any social networking sites. Currier provided information that he had a Dropbox account, listing the username as “scurrier,” the email address associated with the account as “scurrie [REDACTED]@gmail.com,” and the password associated with the account as “[REDACTED].” He indicated that the account was for personal use.

25. On March 22, 2018, I, along with two AUSAs, met with USPO Farwell at the U.S. Probation Office in Concord, NH. During the meeting, USPO Farwell was requested to provide any reports regarding his meetings with Currier related to the incident(s) described above. USPO Farwell advised that he would need to seek approval from the Court prior to disclosing his official notes and/or documentation related to the incident described above. That approval was obtained and USPO Farwell provided certain of his official notes regarding Currier.

26. In that meeting, USPO Farwell was asked to describe in detail what he observed on the above referenced video file he discovered on the Account while using Currier’s Device. Although somewhat repetitive, I am setting out here what USPO Farwell explained during that meeting. Specifically, he said that he had seen an adult female and a pre-pubescent female both nude, visually observing the pre-pubescent female’s breast area. USPO Farwell further explained that the adult female appeared to pull the pre-pubescent female towards her, where the

pre-pubescent then began to suck on the breast of the adult female. USPO Farwell further explained that the adult female then positioned herself on the floor, and appeared to guide the pre-pubescent towards her groin area as if in preparation to have the minor perform oral sex on the adult female. USPO Farwell advised that, at that point, he ceased viewing the video, notified his supervisor of what he observed, and secured the Device.

27. After the meeting with USPO Farwell and pursuant to 18 U.S.C. §2703(f), I submitted a letter to Dropbox, requesting the preservation of all stored communications, records, and other evidence in Dropbox's possession regarding the username and e-mail account that Currier had reported as associated with his Dropbox account.

Information about Dropbox

28. Dropbox is an online service that allows users to store files remotely on Dropbox's servers. Examples of the types of files that may be stored in a user's Dropbox account include documents, images, and videos. The files can be accessed from a user's computer, smartphone, or tablet, or from a Dropbox website.

29. When a user transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the user deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

30. Dropbox is an "offsite" storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and

avoid having the files appear on their computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted only to store them with a service such as Dropbox. These services are often viewed as advantageous for collectors of child pornography because they provide an added level of anonymity and security.

31. Dropbox also allows users to share the files with other individuals by providing a link to their Dropbox account. Users can share individual files, or entire folders containing multiple files.

32. According to Dropbox's privacy policy, posted on April 12, 2017, and available at <https://www.dropbox.com/privacy>, the company collects the following information from a user of its websites, software and services:

a. Information like the user's name, email address, phone number, payment information, physical address and account activity.

b. The user's stored files (such as photos, documents, and emails) and information related to them (such as location tags in photos). If a user gives Dropbox access to the user's contacts, Dropbox will store those contacts on its servers for the user to use.

c. Information from and about the devices the user uses to access Dropbox's services. This information includes IP addresses, the type of browser and device used, the web page the user visited before coming to Dropbox's site, and identifiers associated with the user's devices. Depending on their settings, these devices may also transmit location information to Dropbox.

**Characteristics Common To Individuals Who
Possess, Receive, Or Distribute Child Pornography**

33. Based on my previous experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who view and/or possess, and/or transmit and/or receive images of child pornography:

a. Such individuals often receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they have viewing children engaged in sexual explicit conduct or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

Individuals who have a sexual interest in children or images of children typically retain such images for many years.

b. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer or cellular telephone. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence or inside the possessor's vehicle, to enable the individual to view the child pornography images, which are valued highly.

c. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in

child pornography. Forums, such as chat rooms, bulletin boards, newsgroups or IRC chat rooms have forums dedicated to the trafficking of child pornography images.

34. Based on the information above, I submit that there is probable cause to believe that Scott Currier has possessed child pornography, in violation of 18 U.S.C. §2252, and . I am therefore requesting authority to search (1) the Device and(2) the Account for child pornography and evidence relating to the possession, and distribution of any child pornography.

TECHNICAL TERMS

35. Based on my training and experience, I use the following technical terms to convey the following meanings:

36. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless Device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system (“GPS”) technology for determining the location of the Device.

37. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
38. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage Device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
39. GPS: A GPS navigation Device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation Devices can give a user driving or walking directions to another

location. These Devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

40. PDA: A personal digital assistant, or PDA, is a handheld electronic Device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the Device.

41. Based on my training, experience, and research, and from discussions with others in law enforcement familiar with cellular phone technology, I know that the Device has capabilities that allow it to serve as a wireless telephone, a digital camera, a portable media player, a GPS navigation Device, and a PDA. In my training and experience, examining data stored on Devices of this type can uncover, among other things, evidence that reveals or suggests who possessed and/or used the Device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

42. Based on my knowledge, training, and experience, I know that the Device can store information for long periods of time. The Device is designed to access the Internet and things that have been viewed via the Internet are typically stored for some period of time on internet enabled Devices such as the Device here. This information can sometimes be recovered with forensics tools.

43. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a Device can also indicate who has used or controlled the Device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic Device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic Devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a Device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

44. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

45. *Manner of execution.* Because these warrants seek only permission to examine a Device already in law enforcement's possession, and records from the Account stored under the control of Dropbox, the execution of these warrants does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrants at any time in the day or night.

46. I anticipate executing the warrant for the Account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

47. The description provided by USPO Farwell provides probable cause to believe that at the time he viewed it, Currier's Dropbox account contained material that meets the federal definition of child pornography. Further, the presence of the Dropbox app on the Device and the account information that Currier provided for Dropbox provide probable cause to believe that Currier used the Device to access the cloud-based storage of his Dropbox account, rendering it an instrumentality of the offense of possession of child pornography.

48. The fact that the Dropbox account contained images consistent with those Currier described as located on the Device provides probable cause to believe that the video found in the Dropbox account, or other similar items, will be found stored on the Device. Accordingly, I

submit that there is probable cause to believe that evidence that Currier has possessed child pornography, and has used the Device to do so, may be found on the Device.

49. Based on the foregoing, I submit that there is probable cause to believe evidence of crime, contraband, and fruits of crime, specifically violations of 18 U.S.C. § 2252(a)(4)(B), possession of child pornography, are located on the Device described in Attachment A, and that the Device was an instrumentality of the crime in that it was intended for use, and was used, in committing the crime. I respectfully request that this Court issue a search warrant for the Device, authorizing the seizure and search of the items described in Attachment B.

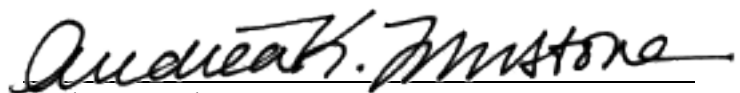
50. I further submit that there is probable cause to believe that evidence of crime, contraband, and fruits of crime, specifically violations of 18 U.S.C. § 2252(a)(4)(B), possession of child pornography, are located in the Dropbox account described in Attachment A, and that the Dropbox account was an instrumentality of the crime in that it was intended for use, and was used, in committing the crime. I respectfully request that this Court issue a search warrant for the Account, authorizing the seizure and search of the items described in Attachment B.

Sworn to under the pains and penalties of perjury.

/s/ Michael Perrella

Michael Perrella
Special Agent
Homeland Security Investigations

Sworn to and subscribed before me this the 23 day of May, 2018.



Andrea K. Johnstone
United States Magistrate Judge

ATTACHMENT A (Phone warrant)

The property to be searched, the Device, is a Samsung Note 8 Model #SM-N950U, currently located in evidence storage at the U.S. Probation Office, 55 Pleasant Street, Concord, NH.

This warrant authorizes the forensic examination of the Device for the purpose of identifying and seizing the electronically stored information described in Attachment B.

ATTACHMENT B (Phone warrant)

All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 2252(a)(4)(B), possession of child pornography including:

1. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, text messages, electronic messages, or other digital data files) pertaining to the production and possession of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
2. In any format and medium, all originals, computer files, and copies of child pornography as defined in 18 U.S.C. § 2256(8) and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), including GPS location data that may show the location at which the image was created or from which it had been sent.
3. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the owner of the Device for the purpose of receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, text messages, electronic messages, and other digital data files) concerning communications between Currier and other parties related to the violations described in the warrant.

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, text messages, electronic messages, and other digital data files) concerning or relating to child pornography or membership in online groups, clubs, or services that provide or make accessible child pornography to members.

6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs, text messages, electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

7. Any and all visual depictions of minors.

8. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, text messages, electronic messages, and other digital data files), pertaining to use or ownership of the Device described above.

9. Any and all documents, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.